METHOD AND APPARATUS FOR ACCESS PARAMETER SHARING

FIELD

[0001] The present invention relates to sharing of access parameters.

BACKGROUND

[0002] Local wireless networks, such as IEEE 802.11 WLANs or wireless wide area networks, are very widely used for Internet connectivity. Majority of private wireless network access points are protected, i.e. they can be hidden and require correct encryption key to be accessed. Various personal communications devices like mobile phones, tablets and laptops are having more and more nomadic users who use their devices increasingly at friends' homes, pubs, cafes and soon also e.g. in private cars. A cellular data connection can be slow, expensive and/or may not be supported.

SUMMARY

[0003] Various aspects of examples of the invention are set out in the claims.

[0004] According to a first embodiment, there is provided a method, comprising: receiving, by an apparatus, a first message from a second apparatus, the first message comprising an information element indicating if access credentials may be requested for the second apparatus, determining, based on the first message, whether access credentials of the second apparatus may be requested, in response to detecting that the access credentials may be requested, transmitting a request message for requesting the access credentials of the second apparatus, and receiving the access credentials from a third apparatus, different from the second apparatus.

[0005] According to a second embodiment, there is provided a method, comprising: receiving, by an access point, a first request message from a non-access point apparatus, transmitting a first response message to the non-access point apparatus, the first response message comprising an information element indicating whether access credentials of the access point may be requested via the access point, after transmission of the first response message, receiving by the access point from the non-access point apparatus a second request message for requesting the access credentials, and transmitting a third request to a third apparatus for transmitting the access credentials to the non-access point apparatus.

[0006] According to a third embodiment, there is provided an apparatus configured to carry out the method of the first and/or second embodiment.

[0007] The invention and various embodiments of the invention provide several advantages, which will become apparent from the detailed description below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0009] FIG. **1** illustrates an example of a wireless communications system;

[0010] FIGS. **2***a* and **2***b* illustrate methods according to some embodiments;

[0011] FIGS. **3***a* and **3***b* illustrate information elements according to an embodiment;

[0012] FIG. **4** illustrates network information sharing architecture according to an embodiment;

[0013] FIG. **5** illustrates a method according to an embodiments; and

[0014] FIG. **6** illustrates a mobile communications device according to an embodiment.

DETAILED DESCRIPTION

[0015] FIG. **1** illustrates an example of a wireless communication system including radio devices, such as devices supporting IEEE 802.11 features. While some wireless network sharing related embodiments are described below with reference to WLANs, it should be appreciated that other embodiments are applicable to sharing access to other wireless networks, such as wireless personal area networks (WPAN), wireless peer-to-peer networks, wireless mesh networks, wireless wide area networks (WAN).

[0016] Mobile devices **10**, **30** may associate with an access point (AP) or a base station **20**. In some embodiments, the devices **10**, **30** are IEEE 802.11 WLAN stations (STA) capable of establishing an infrastructure basic service set (BSS) with the AP **20**. The AP **20** may be a fixed or mobile AP. The AP **20** typically provides access to other networks **50**, e.g. the Internet. In another embodiment, an independent BSS (IBSS) or a mesh BSS (MBSS) is established without a dedicated AP, and in such embodiments the mobile device **10**, **30** may be a non-access-point terminal station. There may also be other WLANs or other types of access networks, such as cellular networks, available for the devices **10**, **30**, via which remote devices **40***a*, such as network servers, may be connected. One or more further local devices **40***b*, in the examples below also referred to as server, may be connected to a locally available wired or wireless network. The system may also comprise other devices, such as tags or sensor nodes **50**.

[0017] The mobile device **10**, referred hereafter as the guest device, may be visiting a coverage area **22** of the AP **20**, which may be owned by a user of mobile device **30**, hereafter referred as the owner device.

[0018] Credentials for accessing a WLAN by establishing a connection with the AP **20** may comprise at least one of a service set identifier, an encryption type indicator, and an encryption key. A Bluetooth address needed for connecting Bluetooth device is an example of a parameter for accessing a WPAN. However, it is to be noted that these are just examples of applicable parameters and the term 'access credentials' is not limited to access parameters of any particular network. An owner of a wireless network often is not willing to share his network and credentials due to security concerns, does not know the required credentials or is not aware how to setup connection credentials into a device. Most people do not want to open their network in order to maintain privacy, to avoid increased traffic on their internet connection or to protect from false accusations of piracy. Some advanced access points support separate guest access but these are not very common. Some expert users also set up a guest network with additional routers and access points. A password protected guest network still requires its owner to share the credentials to guests. It is generally desirable to have an easy and trusted method to give access to protected wireless networks, such as WLAN access points. It may be possible for the owner to authorize or delegate at least some wireless network sharing functions and access credentials provision to another apparatus, such as the server **40***a*, **40***b*. However, a user of a guest